# A view of $x^p+y^p=z^p$ from $x^2+y^2=z^2$

B. L. Ly

## 1. Introduction

Even though Andrew Wiles has proved Fermat's Last Theorem, people still wonder if Fermat had a simple proof as he claimed. How wonderful if Fermat had divulged his proof.

To prove Fermat's Last Theorem, one only needs to investigate impossibility of $x^4+y^4=z^4$ and $x^p+y^p=z^p$, respectively, where $p\geq 3$ is a prime number.

Fermat himself proved impossibility of $x^4+y^4=z^4$ by using his own method of infinite descent. He did not, however, give a proof of impossibility of $x^p+y^p=z^p$.

It was known in India and China more than two millennia ago that $x^2+y^2=z^2$ admits integer solutions. To explain why $x^p+y^p=z^p$ has no integer solutions, we decided to look for a clue in $x^2+y^2=z^2$. The finding reveals if $x^p+y^p=z^p$ is assumed to have integer triplets, z cannot have a lower bound.

## 2. Why $x^2+y^2=z^2$ has integer solutions

It is well known $x^2+y^2=z^2$ has irreducible integer triplets. Three observations can be made:

- One of x and y, say x, is an odd number because G.C.D. (x, y, z)=1.
- Any odd number can be represented by a difference of two squares of relatively prime integers. Therefore, integers z and y can be found such that $x^2=z^2-y^2$.
- z has a smallest integer solution because integers are bounded from below.

If x is an odd number, so is $x^2$. Then, we have $x=m^2-n^2$ and $x^2=a^2-b^2$, where m is relatively prime to n and a is relatively prime to b. With $x=m^2-n^2$, it can be shown $a=m^2+n^2$ and $b=2mn$.

We can choose z=a and y=b to obtain an integer solution triplet:

$$(x, y, z)=(m^2-n^2, 2mn, m^2+n^2) \quad (1)$$

Also, z indeed has a smallest integer solution, which is equal to $2^2+1^2=5$.

We can conclude that the key to $x^2+y^2=z^2$ having integer solutions is x can be an odd number and an odd number can be written as a difference of two squares of integers. Hence integers a and b exist such that $x^2=a^2-b^2$, thereby assuring $x^2=z^2-y^2$ will have integer solutions.

3. Why $x^p+y^p=z^p$, $p\geq3$ being a prime, has no integer solution

Here, we will examine $x^p+y^p=z^p$, $p\geq3$ being a prime number, in the light of $x^2+y^2=z^2$.

Suppose $x^p+y^p=z^p$ has irreducible integer triplets. One of x and y, say x, is an odd number and z must have a smallest integer solution. If x is an odd number, so is $x^p$. Then, $x^p$ has the form:

$$x^p=a^2-b^2=z^p-y^p \quad (2)$$

where a and b are relative primes. Eq. (2) shows $x^p$ is not only a difference of two squares of integers but also a difference of two p-powers of integers.

Integer solution $x^p$ will have a dual form as shown in Eq. (2) if some relatively prime integers c and d exist such that

$$x^p=(c^p)^2-(d^p)^2=(c^2)^p-(d^2)^p \quad (3)$$

Eq. (3) is possible only if both $c=a^{\frac{1}{p}}$ and $d=b^{\frac{1}{p}}$ are integers. If they are, we can choose $c^2$ to be z and $d^2$ to be y. Then, we will have an integer solution triplet for $x^p+y^p=z^p$:

$$(x, y, z)=(x, d^2, c^2) \quad (4)$$

To prove impossibility of $x^p+y^p=z^p$, we choose to show z will descend indefinitely rather than to show $c = a^{\frac{1}{p}}$ and $d = b^{\frac{1}{p}}$ are not integers.

From Eq. (3), $x^p=(c^p)^2-(d^p)^2$ yields

$$x^p=(c^p+d^p)(c^p-d^p) \tag{5}$$

Both $c^p-d^p$ and $c^p+d^p$ are relatively prime because c and d are relative primes.

The integer solution x is either a prime, a power of a prime, or a composite number consisting of mutually prime factors.

Suppose x is a prime or a power of a prime. Because $c^p-d^p$ and $c^p+d^p$ are relatively prime, we have $c^p-d^p=1$, which is impossible because it contradicts $c^p-d^p>1$.

If $x=fg$ is a composite number, with $1<f<g$ and G.C.D. $(f, g)=1$, Eq. (5) results in:

$$d^p+f^p=c^p \tag{6a}$$

$$c^p+d^p=g^p \tag{6b}$$

Both are Diophantine equation also of power p. In Eq. (6a), $c<c^2=z$ violates z is the smallest integer solution. In Eq. (6b), $g<x<z$ also violates z is the smallest integer solution. As z has no lower bound, z cannot be an integer.

4. Conclusion

Suppose $x^p+y^p=z^p$, where $p\geq 3$ is a prime, has integer solutions. Then, x can be an odd number and $x^p$ has a dual form of representation $x^p=a^2-b^2=z^p-y^p$. This dual form was used to show z will descend indefinitely.